Matematinės idėjos ištraukė žmoniją iš olų į civilizaciją

Dokt. Aidas Medžiūnas
Dokt. Vytenis Šumskas

Vilniaus universiteto
Matematikos ir informatikos fakulteto
Taikomosios matematikos institutas

Matematika yra mokslų motina, viena svarbiausių žmonijos civilizacijos kultūros dalių. Naujos matematinės idėjos padeda gilinti suvokimą apie pasaulį ir tobulėti įveikiant gamtos, buities ir visuomenės keliamus iššūkius. Be matematikos iki šiol gyventume olose kaip pirmykščiai žmonės. Šiame straipsnyje pateikiamos kelios matematinės idėjos, leidusios žmonijai žengti platų žingsnį pirmyn ir šių dienų matematikos pasaulyje užimančios itin reikšmingą vietą.


TimeD3-R
180301

Indiškoji skaitmenų sistema yra pirmoji sistema pasaulyje su nulio simboliu, kuris žymi kiekio nebuvimą.

1 pav. (dešinėje) Kreivės ribojamą plotą aproksimuojant vis siauresnėmis figūromis, artėjame prie tikrojo ploto, o tiksliame integralo apibrėžime naudojama begalybė begalinio siaurumo figūrų

Duobutės smėlyje

Daugelis esame įpratę mūsų naudojamą dešimtainę skaitmenų sistemą vadinti arabiškais skaitmenimis. Patys arabai juos vadina indiškais skaitmenimis, nes jie kilo iš Indijos tarp I ir IV a. Bet kadangi indai perdavė šią skaičiavimo sistemą Arabijos tautoms, o jos perdavė europiečiams, šis netikslumas tęsiasi iki pat šių dienų.

Svarbus veiksnys indiškiems skaitmenims įsigalint pasaulyje buvo tas, kad tai draugiškesnė vartotojui sistema nei, tarkime, romėniškoji. Jei norėtume užrašyti du tūkstančius aštuonis šimtus aštuoniasdešimt aštuonis, indiškais skaitmenimis tai bus tik keturi simboliai (2888). Taikant romėniškus skaitmenis prireiks net 14 simbolių (MMDCCCLXXXVIII)! Sudėties, atimties, daugybos ir dalybos veiksmai indiškai atliekami taip pat kur kas lengviau. Kiekvienas antrokas jums stulpeliu prie 2888 pridės 2888. Romėniškai tai nėra taip elementaru, veiksmo atlikimas reikalauja daugiau laiko ir įgudimo.

Arabų šalys, garsėjančios savo pirkliais ir prekyba, sparčiai perėmė indiškus skaičius kaip ekonomiką skatinantį veiksnį. Europoje šiai skaitmenų sistemai įsigalėti prireikė gerokai daugiau laiko. Ji kilo iš Rytų religijų atstovų, o Katalikų bažnyčia, turėjusi ypač daug įtakos Europoje, įtariai žiūrėjo į viską, kas ateidavo iš „netikėlių“ kraštų. Tik pasibaigus viduramžiams, kai bažnyčia prarado didžiąją dalį savo galios, šie skaitmenys galutinai pakeitė romėniškuosius.

Indiškoji skaitmenų sistema yra pirmoji sistema pasaulyje su nulio simboliu, kuris žymi kiekio nebuvimą. Čaturbhudžos (Chaturbhuj) šventykloje Indijoje yra iškaltas seniausias mums žinomas nulio atvaizdas. Pats simbolis kildinamas iš ant smėlio akmenėliais atliekamų skaičiavimų. Skaičiuojant akmenėliai žymėdavo kokį nors kiekį, o juos nuėmus ant smėlio paviršiaus likdavo apskriti pėdsakai, kurie ir įkvėpę nulio vaizdavimą.

Begalinės problemos

Vienas įstabiausių žmogaus intelekto gebėjimų – kurti objektus, kurie peržengia Visatos, laiko ir erdvės ribas. Begalybė yra vienas iš tokių objektų. Su begalybės sąvoka mūsų protai susiduria labai ankstyvame amžiuje. Prisiminkime vaikiškus ginčus:

– Aš turiu šimtą draugų.

– Aš tūkstantį.

– O aš milijoną.

– O aš... milijonų milijoną.

– O aš!.. milijonų milijonų milijonų...

Tokios varžybos baigdavosi tik tada, kai viena iš pusių pavargdavo, bet abu ginčo dalyviai suvokdavo, kad nė vienas negali šio ginčo laimėti, juk skaičiai niekada nesibaigia.

Įtempti žmonijos santykiai su begalybe šiais vaikiškais žaidimais tik prasideda. Ilgą laiką didelę problemą Europos mąstytojams kėlė žmogaus proto atrandamų begalybių suderinamumas su visagalio Dievo vaizdiniu. Jie pastebėjo, kad nors ir kokį didelį skaičių sugalvosime, prie jo pridėję vienetą gausime dar didesnį skaičių. Vadinasi, skaičiai negali turėti ribų ir neįmanoma jų visų žinoti. Bet jeigu Dievas – visagalis, tai jis turi sugebėti suskaičiuoti visus skaičius, nes antraip jis bus ribotas ir egzistuos kažkas už, o gal net virš Dievo. Šią viduramžių teologijos dilemą puikiai apibendrina taip ir neatsakytas žymusis klausimas: „Kiek angelų Visagalis gali sutalpinti ant adatos smaigalio?“

Begalybių pasaulis šiuolaikinėje matematikoje yra kupinas keisčiausių paradoksų ir rebusų. Surikiuokime natūraliuosius skaičius, kuriais skaičiuojame daiktus (1, 2, 3, 4, 5...). Gausime dailią begalinę eilutę skaičių:

1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12...

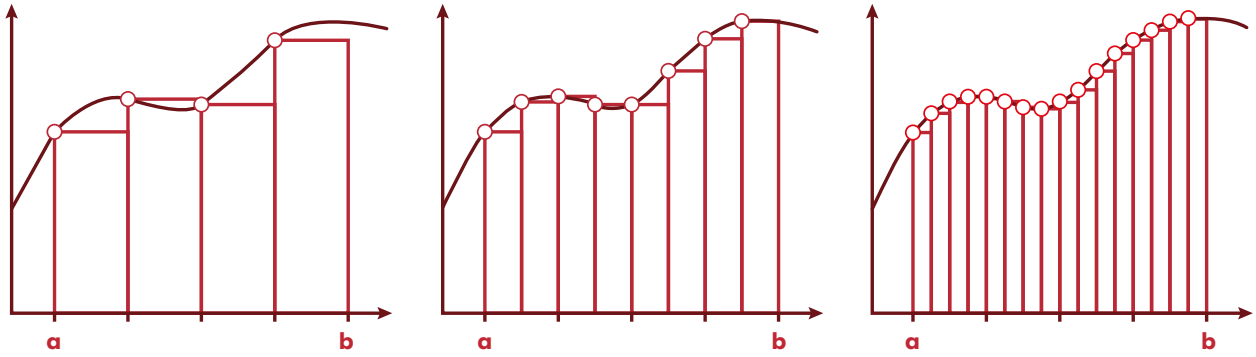
Padauginkime kiekvieną skaičių šioje eilutėje iš 2. Gausime naują begalinę eilutę lyginių skaičių:

2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24...

Pirmojoje ir antrojoje eilutėse skaičių yra po tiek pat, nes antroji eilutė yra ta pati pirmoji, tik padauginta iš 2. Turime dvi skaičių eilutes, kuriose yra vienodas begalinis skaičius elementų. Paradoksas – begalybėje natūraliųjų skaičių yra tokio pat dydžio lyginių skaičių begalybė. Kitaip pasakius – lyginių skaičių yra tiek pat, kiek ir visų natūraliųjų skaičių.

Aukštosios matematikos studijos prasideda nuo integralų

Tai, kas lietuviškai vadinama integraliniu ir diferencialiniu skaičiavimu, angliškai nusakoma vienu patogiu žodžiu – *calculus*. Be šios matematikos šakos neegzistuotų daugybė



modernių matematikos taikymo sričių. Turbūt visiems mokykloje teko spręsti tiesines ir kvadratines lygtis. Jos sudaromos taikant sudėties, atimties, daugybos bei dalybos operacijas ir jų sprendimas nėra itin sudėtingas. Integralinio ir diferencialinio skaičiavimo uždaviniuose turime panašaus pavidalo lygtis, tačiau su papildomomis operacijomis – integralu ir išvestine. Pasitelkus kvadratinę lygtį buvo galima išspręsti nebent elementarų traukinių judėjimo ar tirpalų maišymo uždavinį, o su išvestinių ir integralų lygtimis jau įmanoma spręsti pačius sudėtingiausius uždavinius, kuriuose sąveikauja įvairūs fizikiniai procesai.

Paprastais žodžiais tariant, integralas skaičiuoja figūrų ilgius, plotus, tūrius ir kt., o išvestinė išreiškia greičius, srautus ir daugybę kitų fizikinių charakteristikų. Turėdami kvadratą, žinome elementarią formulę, kaip rasti jo plotą. O jei figūros kraštai nėra lygūs? Tuomet galime pasinaudoti integralu. Formulynuose esančios plotų bei tūrių formulės ir yra išvedamos integruojant. Įstojus į matematikos studijų programą, nuo to ir pradedama – reikia išmokti išsivesti daugybę atmintinai išmoktų formulių.

Pati integralo sąvoka labai sena, pirmąkart aptinkama dar IV a. pr. m. e. Senovės Graikijoje. Tais laikais integralas irgi žymėjo figūros plotą, tačiau skaičiavimai buvo kitokio pobūdžio ir smarkiai apriboti. Prireikė gerų dviejų tūkstančių metų, kol XVII a. nepriklausomai vienas nuo kito Isaacas Newtonas ir Gottfriedas Leibnizas atrado gerokai universalesnį būdą – jei figūros kraštą galime išreikšti per žinomą funkciją, tuomet jos integralą galime rasti analiziškai, remdamiesi paprastomis taisyklėmis. Šių mokslininkų dėka ėmė plisti metodas, leidžiantis lengvai nagrinėti daugybę įvairių fizikinių procesų charakteristikų, o kartu buvo sukurtas tvirtas pagrindas fizikos ir chemijos mokslų plėtrai (1 pav.).

Šifravimas, kurio nenulauš „nedraugiškas“ veikėjas

Per milijonus metų trukusią evoliuciją žmonija išsiugdė ir išpuoselėjo nuostabią priemonę mūsų mintims užkoduoti, perteikti kitam žmogui ir dekoduoti – kalbą. Ji leidžia suprasti įvairių tautų, kultūrų ir kartų žmones ir būti jų suprastiems. Deja, kartais šio kalbos universalumo pasidaro per daug, kai nenorime būti suprasti visų ir visada.

Metodus, kaip sugadinti – pakeisti kalbos universalumą taip, kad žinutės pasiektų tik tam tikrus asmenis, o kitiems jos būtų neperprantamos, vadiname šifravimu, o šifravimo metodus kuriančią ir tyrinėjančią matematikos šaką – kriptografija.

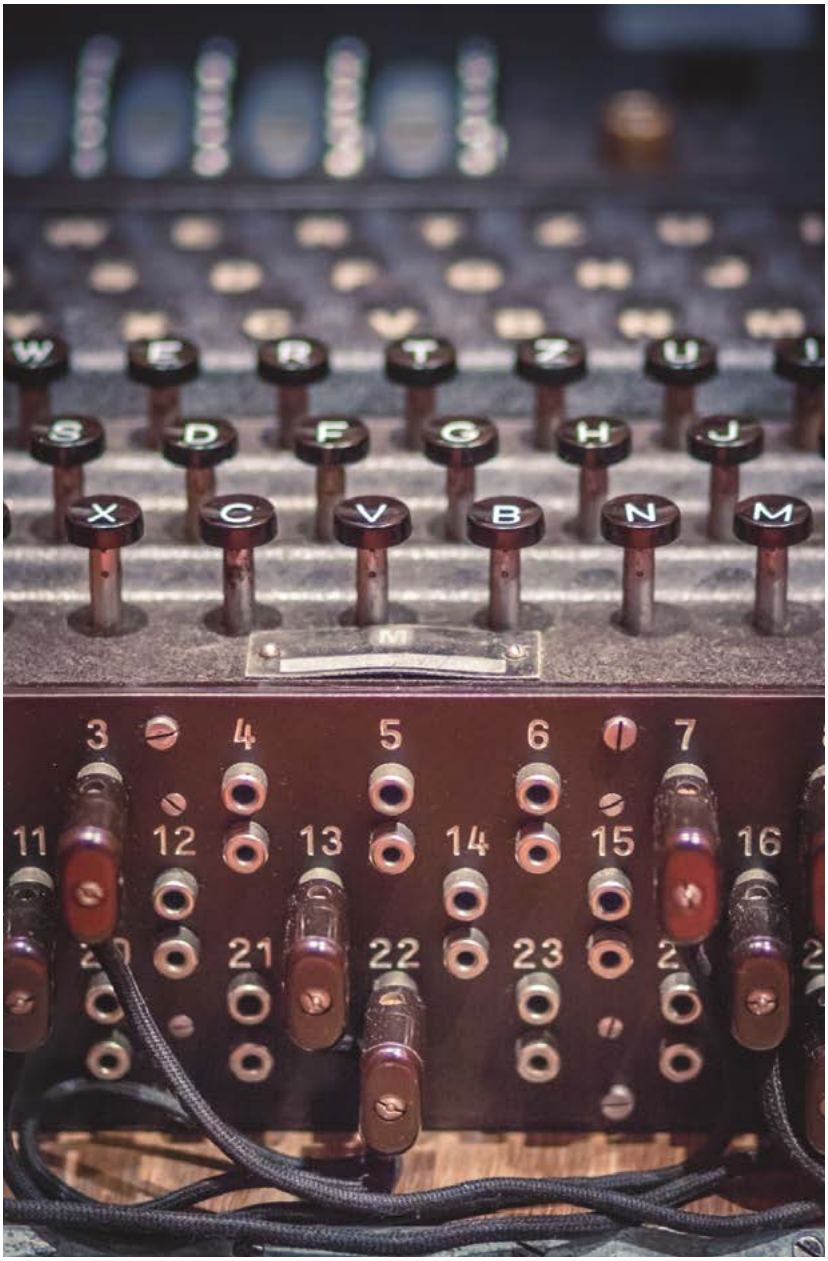
Vienas seniausių šifravimo metodų yra Cezario šifras. Metodo idėja labai paprasta – koduojamas žinutės raides perkeliame per tam tikrą vietų skaičių abėcėlėje. Pavyzdžiui, žodis MATEMATIKA, pakeistas Cezario šifru per tris raides, tampa PCŪFPCŪJNC. Užuot naudoję vieną skaičių, galime naudoti keleto skaičių grandinėlę. Tada žodis MATEMATIKA, pakeistas Cezario šifru per 1–2–3 raides, tampa NBŪĘOCUJLB. Net žymioji Trečiojo Reicho sukurta „Enigma“ buvo tik dar viena Cezario šifro giminaitė, kurioje raidžių perkėlimo tvarkai nustatyti buvo naudojami krumpliaračiai.

Deja, visi klasikiniai šifravimo metodai turi du esminius trūkumus, kurie daro juos neefektyvius. Pirma, sužinojus šifravimo metodą, žinučių iššifravimas darosi nesunkus. Pavyzdžiui, Matematikos ir informatikos fakulteto simbolis LĄUF yra užšifruotas paprastu Cezario šifru – perkėlus visas raides per tam tikrą vietų skaičių. Žmogus iššifruos šį žodį su pieštuku ir abėcėle per kelias minutes, o šiuolaikinis kompiuteris – per tūkstantąją sekundės dalį.

Antra, darant klasikinio tipo užšifravimo metodus sudėtingesnius, laikas, sugaištas siuntėjui koduojant ir gavėjui dekoduojant žinutę, ilgėja. Visą šio straipsnio tekstą žmogui perrašyti perkeliant visas raides per vieną vietą užtruktų iki poros valandų.

Taigi turime gan aiškiai suformuluotą užduotį – norime sukurti šifravimo metodą, kuriuo naudodamiesi greitai ir lengvai galėtume koduoti žinutes taip, kad „nedraugiškas“ veikėjas, net žinodamas, kokiu metodu mes koduojame, negalėtų jų nulaužti. Iš pirmo žvilgsnio atrodo, kad tokio tipo uždavinys yra sunkiai išsprendžiamas. Tačiau XX a. septintojo dešimtmečio matematikams vis dėlto pavyko jį įveikti.

Kiekvienas save gerbiantis trečiokas ar ketvirtokas moka lengvai sudauginti du skaičius. Žinoma, jei skaičiai didesni, gali tekti užtrukti ilgiau, bet



Paprastais žodžiais tariant, integralas skaičiuoja figūrų ilgius, plotus, tūrius ir kt., o išvestinė išreiškia greičius, srautus ir daugybę kitų fizikinių charakteristikų.

apskritai bet kokie du skaičiai sudauginami gan greitai ir lengvai. Dabar pabandykime atlikti atvirkščią užduotį. Kokius du skaičius (nė vienas iš jų negali būti 1) reikia sudauginti, kad gautume 14? 2 ir 7, gerai. O 91? 713? 4087? Galite net naudotis skaičiuotuvais! Jie jums mažai tepadės. Pasirodo, žmonija vis dar nėra sukūrusi jokių greitų ir lengvų metodų, kaip išskaidyti skaičių į jo dauginamuosius (išskyrus paprastą tikrinimą, ar skaičius dalijasi iš konkrečių skaičių). Žinoma, galima naudotis pirminių skaičių (jie dalijasi tik iš savęs ir iš 1) lentelėmis, bet šių skaičių yra begalybė. Dar daugiau, visų pirminių skaičių sąrašo iki didžiausio šiuo metu žinomo pirminio skaičiaus $2^{82,589,933} - 1$ mes net neturime. Vadinasi, jeigu sudauginsite du pakankamai didelius tik jums žinomus pirminius skaičius ir koks nors nedraugiškas veikėjas perims šių skaitmenų sandaugą, jis niekaip negalės greitai (šiuolaikinis nekvantinis superkompiuteris užtruktų keletą milijonų metų) išsiaiškinti, kokius du pirminius skaičius jūs sudauginote.

Šia idėja pagrįstais šifravimo būdais koduojami visi šiuolaikiniai informacijos srautai. Tad kai apsiperkate naudodamiesi internetine bankininkyste, prisijungiate prie elektroninio pašto paskyros ar gaunate programinius atnaujinimus savo telefone, tai vyksta saugiai, nes niekas nežino, kokius du skaičius sudauginote!

Matematikų siaubas – Gödelio teoremos

Jeigu paklaustumėte matematikų, kur slypi matematikos grožis ir stiprybė, dauguma jų vienaip ar kitaip galiausiai pasakytų, kad matematika – mokslas, kuris preciziškai atranda tiesą ir yra apribotas tik žmogaus fantazijos ir intelekto. Kiti tikslieji mokslai turi nepanaikinimas paklaidas, fizinio pasaulio sandaros transformavimo ribas ir kitus neperžengiamus barjerus, o matematika yra laisva tirti ir spręsti bet kokius uždavinius, kokius tik žmogaus protas gali sugal-

voti. Deja, šį nuostabų vaizdinį 1930 m. sugriovė vienas žymiausių visų laikų matematikų Kurtas Gödelis.

Norėdami suprasti Gödelio idėjų fundamentalumą, turime suformuluoti keletą matematinės logikos idėjų.

Pirma, loginę sistemą vadinsime pilna, jei galima įrodyti visus joje esančius teisingus teiginius. Kiekvienas mokslininkas nori tikėti, kad jo mokslas yra pilna loginė sistema, nes tada kiekvienam procesui ir dėsniui galiausiai galima rasti paaiškinimą.

Antra, loginė sistema yra neprieštaringa, jei joje joks teiginys ir jam priešingas teiginys negali būti teisingi vienu metu. Juk braškės tą pačią akimirką negali būti prinokusios ir neprinokusios, o šio straipsnio skaitytojas arba supranta, arba nesupranta, ką skaito.

Apsiginklavę šiais dviem apibrėžimais galime suformuluoti Gödelio nepilnumo teoremas.

Pirmoji Gödelio nepilnumo teorema: kiekviena loginė sistema yra arba nepilna, arba prieštaringa.

Pagalvokime, kokie šios teoremos padariniai. Jeigu loginė sistema yra nepilna, tai reiškia, kad visada atsiras klausimų, į kuriuos mes niekada, jokiais būdais negalėsime toje sistemoje atsakyti. Matematikoje, kaip ir kituose moksluose, egzistuoja hipotezės, kurių žmonija negali išspręsti dešimtmečiais, o kartais ir šimtmečiais. Kai kurios iš jų gali būti (ir turbūt yra) Gödelio teoremos apraiškos ir šimtų mokslininkų bemiegės naktys bei paaukoti gyvenimai buvo pasmerkti nesėkmei nuo pat pirmosios sekundės.

Alternatyva – loginė sistema yra prieštaringa. Iš pirmo žvilgsnio gali pasirodyti, kad ši alternatyva nėra tokia jau baisi. Kas čia tokio, kad koks vienas teiginys ir jam priešingas teiginys yra teisingi vienu metu?

Bėda ta, kad tokioje sistemoje galime įrodyti esant teisingus bet kokius teiginius:

Įsivaizduokime, kad gyvename įprastame mums pasaulyje, vienintelis skirtumas tik tas, kad teiginys *kiaulės moka skraidyti* ir teiginys *kiaulės nemoka skraidyti* yra abu teisingi vienu metu.

Tada teisingas teiginys *kiaulės moka skraidyti arba karvės yra žmogėdros* (nors karvės nėra žmogėdros, bet teiginio pirmoji dalis yra teisinga, tad dėl žodžio *arba* visas teiginys teisingas).

Tačiau mes taip pat žinome, kad kiaulės nemoka skraidyti.

Taigi jau įrodytame teisingame teiginyje *kiaulės moka skraidyti arba karvės yra žmogėdros* pirmajai daliai esant neteisingai, antroji dalis turi būti teisinga ir neskraidančios kiaulės pavertė karves žmogėdromis.

Šį paradoksalų prieštaringos sistemos elgesį vadiname dedukciniu sprogimu.

Bijodami dedukcinio sprogimo ir karvių žmogėdrų, matematikai renkasi tikėti, kad matematika yra neprieštaringa sistema. Taip, teisingai perskaitėte – TIKĖTI, nes Gödelis įrodė dar vieną teoremą-prakeiksmą.

Antroji Gödelio nepilnumo teorema: neprieštaringa loginė sistema negali įrodyti savo neprieštaringumo.

Nors tūkstantmetė žmonijos patirtis rodo, kad matematikoje nėra prieštaringų teiginių, mes niekada galutinai to negalėsime įrodyti matematinėmis priemonėmis.

Šios teoremos gali pateikti labai liūdną ir pilką matematikos ir viso mokslo perspektyvą – žmonija turi susitaikyti gyventi su nepilnumo vilku, nes tik taip GAL neužšoks ant prieštaringumo meškos. Tačiau Gödelio teoremos veikia tik tų pačių sistemų viduje. Vadinasi, mes galime atsakyti į visus mums rūpimus klausimus, bet tam turime sukurti dar platesnes, dar turtingesnes logines sistemas ankstesnėms sistemoms paaiškinti. Na, o paaiškinę senąsias sistemas – kurti dar naujesnes, dar turtingesnes sistemas naujoms problemoms aiškinti.

Matematika nėra pasaka su laiminga pabaiga, tai pasaka be galo.

Nors tūkstantmetė žmonijos patirtis rodo, kad matematikoje nėra prieštaringų teiginių, mes niekada galutinai to negalėsime įrodyti matematinėmis priemonėmis.